National Cyber Security Centre
Ministry of Justice and Security

Your remote work systems have become essential

What do you do when your remote work software fails?

Factsheet FS-2020-02 | version 1.1 | 13 April 2020

Many organisations have instructed their employees to work from home after the introduction of the COVID-19 measures. This has made the availability of remote work systems mission-critical for these organisations. Any previous risk analyses about this availability are probably no longer sufficient.

NCSC-NL recommends that you identify the critical processes in your organisation and that you take measures to manage availability risks. The extensive action perspective at the end of this factsheet helps you prepare your organisation for this scenario.

Background

After the introduction of the measures to mitigate COVID-19, many organisations have instructed their employees to work from home. By doing this, organisations can keep working without exposing their employees to additional risk of infection. This also enables employees to take care of their children during school hours, as many of them currently need to do.

Target audience

Chief information security officers (CISO's), IT managers, security officers

The following parties have contributed to this factsheet:

- Dutch Tax and Customs Administration
- National Communications Security Agency (NBV) (part of the General Intelligence and Security Service)
- Rabobank
- Schuberg Philis
- de Volksbank

In January, NCSC-NL recommended that organisations turn off their Citrix remote work systems.[1] Many organisations that used Citrix to enable their employees to work from home, decided to act on this advice, due to a serious vulnerability in this software. The vulnerability that led to the advice in January was by no means unique.[2] All software contains programming errors, and all remote work software could contain a similar vulnerability. However, the associated advice, to stop working from home, is not feasible under the current circumstances.

What is the situation?

The availability of many remote work systems is suddenly mission-critical for organisations, due to the enormous increase in the number of people that work from home. Even if a disruption in your remote work software would earlier be considered a minor risk, such a disruption would currently pose a major threat.

Previous risk analyses concerning the availability of your remote work systems are probably insufficient. After all, these risk analyses did not take into account that organisations would rely on employees working from home during the COVID-19 outbreak. Measures based on these risk analyses will fall short of ensuring the availability of your remote work systems in the current situation.

Supporting ICT processes, such as the issuance of laptops, tokens and other physical ICT resources, are often carried out in a limited fashion now. There is less IT personnel available at the office to attend to these processes. Furthermore, issuing such resources may pose additional COVID-19 infection risk. This motivates organisations to keep the issuance of such resources limited.

What are the risks?

If a serious vulnerability in your remote work software were to be discovered, your organisation is faced with a dilemma. If you do nothing, you are allowing attackers unfettered access to your ICT. If you do intervene and switch off remote work systems, you are risking the continuity of your organisation. For most organisations, both scenarios are simply unacceptable.

Other scenarios also pose a risk to the availability of your remote work systems. Examples include overload due to a sharp increase in the number of users, a shortage in the number of licenses or accounts, DDoS attacks on the access points of your network, or unintentional disruptions in the underlying systems. All these risks already existed before the large-scale outbreak of COVID-19, but their impact has since increased significantly.

Operational cyber security: another critical process

When identifying your critical processes, keep in mind that these processes themselves also depend on certain things. More specifically, we call your attention to maintaining your operational cyber security processes, such as incident response and network monitoring. After all, your organisation uses these processes to manage the risks that arise when processes are performed in an alternative way. Therefore, it will remain necessary to perform operational cyber security processes, possibly in a slimmed-down fashion.

If remote work systems are no longer available, employees will be inclined to use other familiar software they use in their personal life. Well-known examples are free email services and cloud platforms for collaboration and file sharing. If your employees use such software outsite the regular risk management processes, it could lead to serious additional security risks, such as information leakage. In some cases, you might be able to accept the use of such services, if it helps you to avert a greater evil. By already thinking about the use of such services, you are able to make a considered choice if your remote work systems become unavailable, and to communicate this decision clearly to your employees. The action perspective provides further recommendations.

What does NCSC-NL recommend?

NCSC-NL recommends that you identify the critical processes of your organisation and that you take measures to manage availability risks. Of course, all parts of your organisation are important, but it is simply too costly to keep everything running in the case of a serious disruption. By concentrating on the activities that are strictly necessary for the organisation's goals, you ensure focused attention on the aspects that really count.

For each of your organisation's critical processes, determine to which extent it leans on remote work systems. For example, are employees currently using a collaboration space, webmail or a remote desktop to perform this process? Make a list of all remote work systems that are important to one or more critical processes. Of course, a critical process depends on more than just remote work systems. However, this advice assumes that appropriate measures for other ICT systems were already in place before the COVID-19 outbreak. If a system played a key

[1] See https://english.ncsc.nl/latest/news/2020/january/20/install-patches-for-citrix-adc-en-citrix-gateway-servers.

[2] See e.g. https://www.ncsc.nl/actueel/nieuws/2019/oktober/18/pulse-secure-en-fortigate-nog-veel-organisaties-in-nederland-kwetsbaar (only available in Dutch).

role in a critical process before the COVID-19 outbreak, regular risk management would have already led to appropriate measures being taken.

Make an inventory of the availability risks for the remote work systems upon which critical processes depend. Which problems are foreseeable in each of these systems, and how would this risk threaten the performance of the critical processes that depend on the system?

Next, take measures to manage the identified risks. These measures will be in one of two categories. On the one hand, you will take measures to better secure existing systems, and on the other hand you will take measures that make your critical processes depend less on the availability of these remote work systems. The action perspective provides examples of such measures.

Action perspective

Step 1: Identify the critical processes of your organisation.	- A process is considered critical if a disruption would quickly be a threat to the organisation's goals. - Don't fall into the trap of designating too many processes as critical. It really is necessary that you choose. The fewer processes you designate as critical, the more attention you can give to those that really count. - Do you have many processes that are important? It may be helpful to rank them internally. For example, you might gauge the priority of a critical process to be 'average', 'high' or 'top'. This will help you prioritise measures in later steps. - Some processes can be made less critical with additional measures. For example, you might be able to postpone certain services if you communicate proactively to internal or external stakeholders.
Step 2: Determine to what extent critical processes depend on remote work systems.	- Study each critical process carefully, and determine which remote work systems are currently used to perform this critical process. - Determine to what extent this critical process could be performed unchanged if these remote work systems are unavailable. Ideally, this would happen through established and tested procedures, but under the current circumstances, any way 'in which it could work' would already be welcomed. - Make a list of the remote work systems that are essential for every critical process.
Step 3: Identify availability risks of the remote work systems upon which critical processes depend.	- Use the risks that are enumerated in the 'What are the risks?' section. Complement these with risks that are specific to your situation, for example as determined in previous risk analyses.
Step 4: Take measures to manage the identified risks: try to prevent unavailability, and make sure you're ready if disruption does happen.	Take additional measures for existing remote work systems. - *Example* Ensure that you have the right support contract for your remote work software. If you immediately need help in case of an outage or other problems, a basic-level contract might not suffice. Determine how soon you would need help, and what type of help you need. Check whether the arrangement you have with your vendor still satisfies your needs. - *Example* For each user, track the IP addresses from which he or she connects to your network, or establish a procedure to allow users to quickly determine their IP address and pass it along to you. Should a serious vulnerability present itself in your remote work software, you will be able to keep your remote work software online with the use of IP whitelisting. This allows you a bit more time to determine the next steps. - *Example* Purchase sufficient capacity. Most organisations have not originally built their remote work systems to handle the large number of users currently using them. Consider whether the size of your remote work systems still befits the current use, for example in the number of accounts, the number of licences or the required bandwidth. - *Example* Take anti-DDoS measures on the access points of your remote work systems. A DDoS attack is easy to perform. If your remote work systems cannot handle that, it will quickly lead to availability

problems. More advice on anti-DDoS measures is available in the NCSC-NL factsheet 'Technical measures for the continuity of online services'.[3]

Establish alternatives for your remote work systems to support critical processes.

- *Example* Create a second access point, based on software from a different vendor. This works especially well for VPN-based access, because the data traffic does not essentially change when using a VPN from a different vendor. For example, you might choose to already provide employees who are involved in critical processes with access through this second access point, thus making it easier for them to switch.
- *Example* Some applications can be made available directly over the internet, without any portal or VPN. If you choose this option, take into account that these applications will contain vulnerabilities, and that an attacker can now reach them more easily. Therefore, combine this measure with IP whitelisting if possible, as explained in the additional measures for existing remote work systems.
- *Example* Create the means to perform critical processes in the office in small teams. Not every critical process is suited to be performed by an employee who works from home. If you ask employees to come to the office, take measures to mitigate COVID-19 infection risks. Put together several teams that, if necessary, can take over for each other. You might want to already draft schedules for these teams, to ensure that employees are available on short notice. You might choose to keep some employees out of the teams, as a backup. Ensure strict physical separation between the teams. Take necessary hygiene measures in the office, to prevent infection by colleagues or through surfaces if at all possible.
- *Example* Identify the risks of using services intended for personal use, and advise your employees on their use. You may be able to keep performing some processes by switching to such alternative ICT resources. Examples include popular services for file sharing and personal email. Identify the risks if this were to happen, and weigh those risks against the consequences of a disruption of your process. Draft clear guidelines on using these resources relatively securely. The NCSC-NL factsheet 'Choosing a messaging app for your organisation'[4] outlines this approach in the messaging app context. The advice given there applies to other types of services as well.
- *Example* Prepare a roadmap and communications for when remote work systems are no longer available. For example, some employees will no longer be able to work. Instruct them to actually stop working, to ensure that they don't use personal ICT resources to keep working in an ad hoc fashion. In the roadmap, describe the steps necessary to switch to alternative resources. Keep in mind that some means of communication will not be available at that time.

[3] See https://english.ncsc.nl/publications/factsheets/2019/juni/01/technical-measures-for-the-continuity-of-online-services.
[4] See https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-choosing-a-messaging-app-for-your-organisation.

Publication
National Cyber Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2020-02 | version 1.1 | 13 April 2020